

AB:JV  
F# 2018R02044

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF  
THE PREMISES KNOWN AND  
DESCRIBED AS 82-50 235<sup>th</sup> STREET,  
QUEENS, NY 11427

APPLICATION FOR A SEARCH  
WARRANT FOR A PREMISES AND  
CLOSED OR LOCKED CONTAINERS,  
COMPARTMENTS AND ELECTRONIC  
DEVICES FOUND THEREIN

Case No. 19-M-989

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, CHRISTINE A. CULLEN, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search: the premises known as 82-50 235<sup>th</sup> Street, Queens, NY 11427, including a freestanding garage at that address, and any closed or locked containers, compartments and electronic devices contained therein (the “TARGET PREMISES”) as described in Attachment A(I), for the things described in Attachment A(II).

2. I am a Postal Inspector with the United States Postal Inspection Service (“USPIS”) and have been since June 2017. During my time as a federal law enforcement officer, I have personally participated in numerous investigations and arrests, the debriefing of witnesses and the execution of numerous search warrants, including the execution of search warrants for electronic devices, including cellular telephones and internet-capable devices

contained therein. I am familiar with the facts and circumstances set forth below from: (a) my participation in the investigation; (b) my review of the investigative file and reports of other law enforcement officers involved in the investigation; (c) my review of bank records, telephone records, social media accounts and other sources of information; and (d) my conversations with other law enforcements officers, including law enforcement officers executing the search warrant upon 82-51 234<sup>th</sup> Street, Queens, New York 11427 on October 23, 2019.

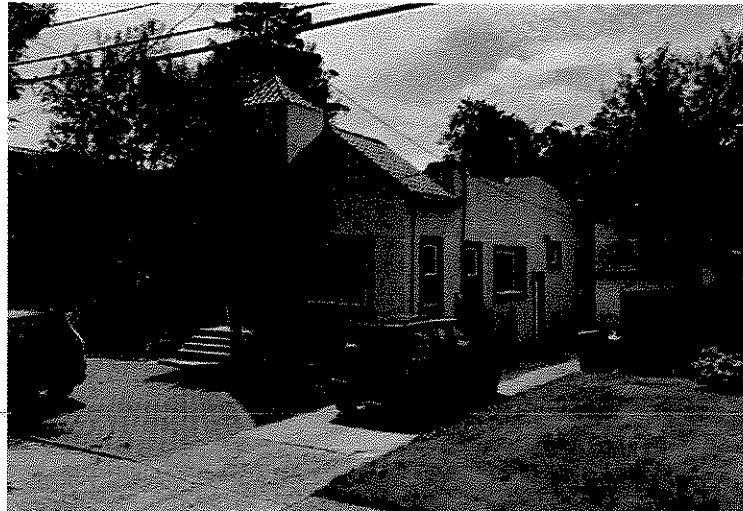
3. Upon information and belief, there is probable cause to believe that there is kept and concealed within the TARGET PREMISES items that constitute evidence, fruits and/or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 402 (Contempt), 542 (Entry of Goods by False Statement), 545 (Smuggling), 554 (Smuggling Goods From the United States), 1001 (False Statements or Entries Generally), 1341 (Mail Fraud), 1343 (Wire Fraud) and 1349 (Attempt and Conspiracy), and 21 U.S.C. §§ 331 (Food Drug and Cosmetic Act Prohibited Acts), 352 (Misbranded Drugs), and 355 (New Drugs) (collectively, the “SUBJECT OFFENSES”).

4. Unless specifically indicated, all conversations and statements described in this affidavit are related in sum and substance and in part only. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

---

**THE TARGET PREMISES**

5. The TARGET PREMISES is 82-50 235<sup>th</sup> Street, Queens, NY 11427, a green one-story single-family residence with a red brick driveway, including a freestanding one-car garage with a white garage door located to the rear of the residence, and any closed and locked compartments and containers, cellular telephones and internet-capable devices contained therein. Photographs of the front of the TARGET PREMISES are shown below:



6. Public records checks show that the TARGET PREMISES were owned by JASON VALE from November 15, 1999, to October 30, 2018, when the property was transferred to the Barbara Vale Revocable Trust. BARBARA VALE is JASON VALE's mother. BARBARA VALE AND JASON VALE (collectively, the "VALES"), together with others, are the targets of violations of the SUBJECT OFFENSES. Based on my review of law enforcement records, JASON VALE is believed to be unmarried. Based on surveillance, JASON VALE is believed to occupy the TARGET PREMISES alone. Based on my review of law enforcement records as of October 22, 2019, I have learned that utilities of the TARGET PREMISES, including bundled cellular phone and internet services, are registered in JASON VALE's name.

7. For the reasons detailed below, there is probable cause to believe that the TARGET PREMISES, including the electronic devices contained therein, contains evidence, fruits and instrumentalities of the SUBJECT OFFENSES.

### **PROBABLE CAUSE**

#### **A. Background Regarding Sale of Laetrile and Similar Products**

8. Based on my investigation, I know that there is an active market for products that have not been approved by the U.S. Food and Drug Administration ("FDA"), but that sellers nonetheless market as being able to treat and cure diseases, including cancer. One of these products is amygdalin. Amygdalin is a glucoside found in the kernel or seeds of most fruits and is frequently referred to as "Laetrile" or "Vitamin B-17." While some people believe that Laetrile can treat and control cancer, the FDA does not support this claim. Additionally, there are no published clinical studies supporting the claim that Laetrile is safe or effective.

Thus FDA does not support the use of Laetrile for the treatment of cancer. Moreover, the medical community has found that cancer patients who nonetheless utilize Laetrile often forgo conventional therapies to their detriment, thus presenting a health risk. Accordingly, it is a violation of the Food Drug and Cosmetic Act to promote unapproved and misbranded drugs as a cure for any disease, including cancer.

B. Legal Proceedings

9. In 1999, the government filed a civil action against JASON VALE, an individual, and his company Christian Brothers Contracting Corporation, a corporation, alleging that they were distributing Laetrile as a cure for cancer and seeking, inter alia, that they be permanent enjoined from selling or promoting Laetrile as a cure for cancer in the future (the “Civil Action”). (No. 99 CV 7683.)

10. On April 20, 2000, Vale, Christian Bros. and their attorneys appeared at the hearing on the government’s motion for a preliminary injunction. At that time they offered no evidence or legal arguments to suggest that the government was not entitled to a preliminary injunction; to the contrary, they consented to the issuance of a preliminary injunction.

11. On November 17, 2000, the Honorable John Gleeson approved a Consent Decree of Permanent Injunction (the “INJUNCTION”) permanently restraining and enjoining JASON VALE, Christian Bros. Contracting Corp. “and each and all of their agents, representatives, employees, successors and assigns, and any and all persons in active concert or participation with any of them” from *inter alia*:

Introducing or delivering for introduction into interstate commerce, holding or sale after shipment in interstate commerce, manufacturing, processing, packing, labeling, promoting in violation of the FDC Act, or distributing amygdalin, laetrile, “Vitamin B-17”, apricot seeds, any



similar product containing or purporting to contain amygdalin, laetrile, “Vitamin B-17”, or apricot seeds, or any drug product that is a new drug as defined in 21 USC 321 (p)....”

12. Despite entering into the INJUNCTION, JASON VALE and Christian Bros. Contracting Corp. continued to sell amygdalin, laetrile, Vitamin B-17, apricot seeds and similar products (the “Enjoined Substances”) in violation of the INJUNCTION.

13. On April 16, 2002, based upon the affidavit of a special agent of the FDA, the district court initiated a criminal contempt prosecution against JASON VALE by issuing an order to show cause. The order to show cause charged JASON VALE with four counts of criminal contempt in violation of 18 U.S.C. § 401(3): (1) that, with the intent to deceive the FDA, the district court and his customers, JASON VALE labeled, packed and distributed laetrile in violation of the preliminary injunction in the Civil Action; (2) that, with the intent to deceive the FDA, the district court and his customers, JASON VALE labeled, packed and distributed laetrile in violation of the permanent injunction in the Civil Action (Count Two); (3) that JASON VALE promoted laetrile as a cure for cancer over the Internet in violation of the preliminary injunction in the Civil Action (Count Three); and (4) that JASON VALE promoted laetrile in violation of the FDCA as a cure for cancer over the Internet in violation of the permanent injunction in the Civil Action (Count Four).

14. On July 21, 2003, JASON VALE was convicted after a trial before Judge Gleeson of three counts of criminal contempt, which stemmed from his violations of the express terms of the INJUNCTION issued by Judge Gleeson. (No. 02 CR 466, ECF No. 83.) Thereafter, Judge Gleeson sentenced JASON VALE to 63 months’ incarceration. (ECF No.

128.) In 2005, the Second Circuit affirmed Jason Vale's convictions. United States v. Vale, 140 F. App'x. 302 (2d. Cir. 2005).

15. On February 2, 2005, in response to a pro se motion for "clarification" of the INJUNCTION filed by JASON VALE, Judge Gleeson observed:

I find the application troubling. First, Vale has demonstrated great familiarity (but not great compliance) with the statutes and regulations at issue in this case. He can read the relevant provisions of the FDC Act himself for a reminder of the conduct he agreed would be prohibited by the consent decree. Second, give the extensive, lucrative and fraudulent conduct that gave rise to Vale's contempt conviction, the last endeavor he should be planning is the promotion of laetrile products in any way.

(No. 99 CV 7683, ECF No. 40.)

C. October 22, 2019 Search Warrant on 82-51 234<sup>th</sup> Street, Queens, NY 11427

16. On October 22, 2019, the United States filed an Application for a Search Warrant for a Premises and Closed or Locked Containers, Compartments and Electronic Devices Found Therein for the Premises Known and Described as 82-51 234<sup>th</sup> Street, Queens, NY 11427, which is the residence of BARBARA VALE and is directly behind the TARGET PREMISES, a copy of which is attached to and incorporated herein as Attachment B.

17. Also on October 22, 2019, the Honorable Sanket J. Bulsara issued a Search and Seizure Warrant In the Matter of the Search of the Premises Known and Described as 82-51 234<sup>th</sup> Street, Queens, NY 11427, a copy of which is attached to and incorporated as Attachment C (hereinafter the "234<sup>th</sup> Street Search Warrant").

18. On the morning of October 23, 2019, federal law enforcement agents executed the 234<sup>th</sup> Street Search Warrant. During the execution of the 234<sup>th</sup> Street Search Warrant, the agents found five 5-gallon orange Home Depot buckets in BARBARA VALE's

garage and 15 5-gallon in her home. The New York Department of Environment Protection (“NYDEP”) has identified the contents of the 20 5-gallon buckets as Dimethyl sulfoxide (“DMSO”).

19. The NYDEP has advised law enforcement personnel that the DMSO present at the premises is a flammable hazard.

20. In addition, from the rear of the 82-51 234<sup>th</sup> Street location, law enforcement personnel have an unobstructed view of the rear of the TARGET PREMISES, including the backyard and a screened-in porch. From that vantage, law enforcement personnel can see two black approximately 55-gallon plastic drums in the backyard (the “55-gallon drums”) and approximately seven to ten 5-gallon orange Home Depot buckets inside of the screened-on porch of the TARGET PREMISES.

D. October 23, 2019 Arrest of Jason Vale

21. On October 22, the United States filed a criminal Complaint naming JASON VALE and BARBARA VALE as defendants. (19-MJ-969.) In connection with that action, the Court issued Arrest Warrants for JASON VALE and BARBARA VALE.

22. On the morning of October 23, 2019, federal law enforcement agents arrested JASON VALE at the TARGET PREMISES. During the arrest of JASON VALE, law enforcement agents detected a strong garlicky sour smell. After arresting JASON VALE and advising JASON VALE of his Miranda rights, law enforcement officers asked the source of the smell, and JASON VALE responded “It is DMSO. I use it.”

23. Law enforcement officers also asked JASON VALE if he consented to a search of the two 55-gallon drums in the backyard of the TARGET PREMISES. JASON



VALE refused to provide consent, stating that it was not his property, but informing law enforcements agents that one of the barrels contained DMSO, which he asserted was not flammable, and that the other barrel was empty.

E. Use of WEBSITE to Sell DMSO

24. As set forth in greater detail in Attachment B, the Application for a Search Warrant for a Premises and Closed or Locked Containers, Compartments and Electronic Devices Found Therein for the Premises Known and Described as 82-51 234th Street, Queens, NY 11427, since at least January 2013, JASON VALE and BARBARA VALE (collectively, the “VALES”) have been operating an online business through a website called “Apricotsfromgod.info” (the “WEBSITE”), from which consumers may purchase various products.

25. As recently as today, the VALES sell 2 oz. and 8 oz. bottles of DMSO on the WEBSITE for \$14.00 and \$38.00 respectively.

26. The WEBSITE states in part:

“Always have a bottle ready in the medicine cabinet. Our DMSO is the highest grade available. Pharma Grade, not industrial grade. (Industrial grade is not toxic or anything, however we supply a more pure form[.])

...

DMSO can be used for a multitude of things, from saving yourself from paralysis after a stroke by orally ingesting every 15 minutes to break up the clot, to sinus infections (nose dropper of DMSO). It also works for high eye pressure (drop it in your eye), swollen ankles due to a sprain (will take down swelling within 5 minutes) shoulder pains and all joint problems and much more. The book “Nature’s Healer” has over 300 pages of the uses of DMSO. If I were a snake oil salesman with DMSO, the towns would have been waiting in line for days

before my ... It is used as a solution when an organ is waiting for a transplant.

...

DMSO will help the body stop a stroke as it is happening

...

Those with neck and spinal injuries receiving DMSO treatment directly after the injury may never be paralyzed and will definitely be less paralyzed if any. Prompt use of DMSO after a heart attack prevents much damaging of the heart muscle.

...

It can be used on any type of cold sore.

...

Bursitis of the shoulder will clear up after 30 days of use.

...

Injected under the bark of a sick tree, the tree will become youthful again.

27. The Food and Drug Administration has not authorized DMSO as a drug for the treatment of the medical conditions listed in paragraph 26 supra.

#### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

28. As described above and in Attachment A(II), this application seeks permission to search for records that might be found on the TARGET PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

---

29. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating

system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files.

Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
- e. Based on actual inspection of other evidence related to this investigation, including electronic mail, the WEBSITE, invoices, and home-generated “Click-N-Ship” postage and mailing labels, I am aware that computer equipment was used to generate and transmit documents used in the VALEs’ business importing and selling Laetrile and similar products. There is reason to believe that there is a computer system currently located on the TARGET PREMISES.

30. *Forensic evidence.* As further described in Attachment A(II), this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the TARGET PREMISES because:

- a. ~~Data on the storage medium can provide evidence of a file that was once on the~~  
storage medium but has since been deleted or edited, or of a deleted portion of

a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a

residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatng or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's



state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators.

Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence
-

or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

31. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

**REQUEST FOR AUTHORIZATION TO DESTROY DMSO**

33. It is respectfully requested that this Court authorize the destruction of the DMSO seized from the TARGET PREMISES and from 82-51 234th STREET, QUEENS, NY 11427.

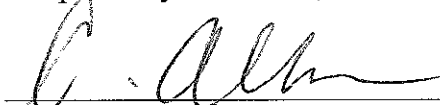
34. As set forth supra in paragraph 19, NYDEP has advised law enforcement personnel that the DMSO present at the premises is a flammable hazard.

35. In addition, the Materials Safety Data Sheet for DMSO states that DMSO is “considered hazardous by the 2012 OSHA Hazard Communication Standard (29 CFR 1910.1200)”. The Safety Data Sheet also categorizes DMSO has a Category 4 Flammable Liquid, and makes the Hazard Statement that it is a “Combustible liquid.” A copy of the Safety Data Sheet is included as Attachment D.

CONCLUSION

36. I submit that this affidavit supports probable cause for a warrant to search the TARGET PREMISES described in Attachment A(I), including any closed containers, locked compartments and electronic devices found therein, and seize the items described in Attachment A(II).

Respectfully submitted,




CHRISTINE A. CULLEN

Postal Inspector

United States Postal Inspection Service

Subscribed and sworn to before me on October 23, 2019

  
Honorable Sa  
UNITED STATES

LLD 11  
S/Bulsara

E

## ATTACHMENT A

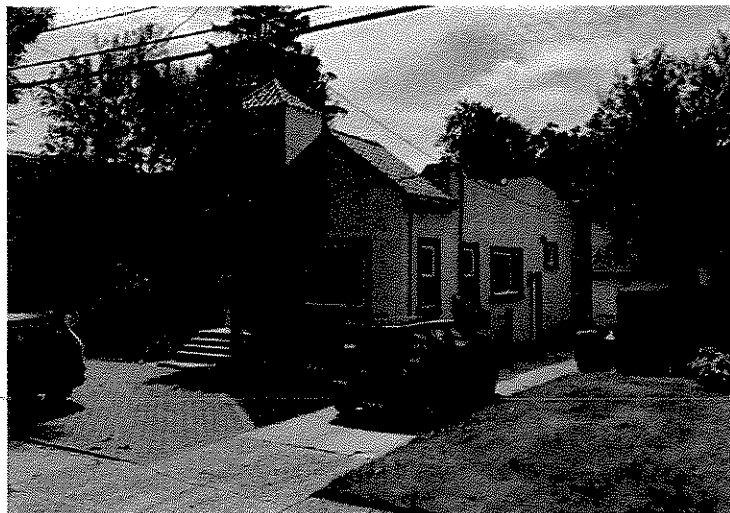
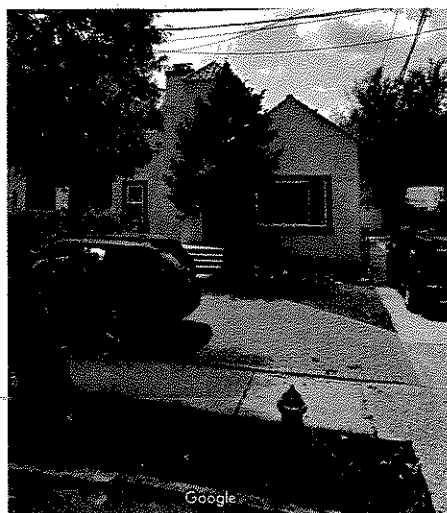


## ATTACHMENT A

### I. Premises to be Searched—Target Premises

The premises to be searched (the “Target Premises”) are described as follows, and include any closed or locked containers, compartments and electronic devices (including computers, cellular telephones and internet-capable devices) and storage media found therein:

the green one-story single-family residence with a red brick driveway, including a freestanding one-car garage with a white garage door located to the rear of the residence, located at 82-50 235<sup>th</sup> Street, Queens, NY 11427, as shown in the photographs below:



## **II. Items to Be Seized**

### **A. Evidence, Fruits, and Instrumentalities of the Subject Offense**

The items to be seized from the Target Premises include the following evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 402 (Contempt), 542 (Entry of Goods by False Statement), 545 (Smuggling), 554 (Smuggling Goods From the United States), 1001 (False Statements or Entries Generally), 1341 (Mail Fraud), 1343 (Wire Fraud) and 1349 (Attempt and Conspiracy), and Title 21, United States Code Sections 331 (Food Drug and Cosmetic Act Prohibited Acts), 352 (Misbranded Drugs), and 355 (New Drugs) (“Subject Offenses”), described as follows:

a. Evidence of the ownership, control and use of the Target Premises, including bills, mail envelopes, addressed correspondence, bank statements, and identification documents.

b. Evidence concerning introducing – or delivering for introduction – into interstate commerce, holding for sale after shipment in interstate commerce, manufacturing, processing, packing, labeling, promoting in violation of the Federal Food, Drug, and Cosmetic Act (FDC Act), 21 U.S.C. §§ 301-97, or distributing amygdalin, laetrile, “Vitamin B-17,” apricot seeds, any similar product containing or purporting to contain amygdalin, laetrile, “Vitamin B-17,” of apricot seeds, or any drug product that is a new drug, as defined in 21 U.S.C. § 321(p) (the “Enjoined Substances”), and as enjoined by the Court’s 2000 Consent Decree of Permanent Injunction, including but not limited to:

- Enjoined Substances;
- Dimethyl sulfoxide (DMSO), and any containers containing Dimethyl sulfoxide (DMSO);
- correspondence concerning the purchase, shipping, testing, labeling, packaging, transport and sale of Enjoined Substances;
- labeling and packaging materials for Enjoined Substances;
- books, records, receipts, notes, ledgers and other papers relating to Enjoined Substances.

c. Evidence concerning introducing – or delivering for introduction – into interstate commerce any drug that is misbranded within the meaning of 21 U.S.C. §§ 352(c), 352(f)(1), or 353(b)(1).

d. Evidence concerning causing the misbranding, within the meaning of 21 U.S.C. §§ 352(c), 352(f)(1), or 353(b)(1), of any drug while held for sale after shipment in interstate commerce.

e. Address and/or telephone books, rolodex indices and any records (paper or electronic) reflecting names, addresses, telephone numbers, and email addresses, and insurance information of customers who purchased or were shipped Enjoined Substances.

f. Contact information and communications with co-conspirators including telephone logs, text messages, messages sent through encrypted applications, emails, and hand written notes.

g. United States or foreign currency, money wrappers, checks, jewelry, precious metals, and other valuables used to purchase Enjoined Substances, or which represent the proceeds of the Subject Offenses.

h. Passwords and keys necessary to obtain access to closed or locked containers, compartments or electronic devices.

#### **B. Search and Seizure of Electronically Stored Information**

The items to be seized from the Target Premises also include any electronic devices (including computers, cellular telephones and internet-capable devices) and storage media that may contain any electronically stored information falling within the categories set forth in Section II.A of this Attachment above, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners. In lieu of seizing any such electronic devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be seized from the Target Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

#### **C. Review of ESI**

Following seizure of any electronic devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Sections II.A and II.B of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

## ATTACHMENT B